(19) Japan Patent Office (JP)
(11) Laid Open Patent Application
(12) Public Patent Bulletin (A)
HEI3[1991]-185585
(43) Laid open August 13, 1991 (Heisei 3)
(51) Int. Cl.[5] Identification Symbol
Office reference number
G 06 K 17/00 S 6711-5B
G 07 F 7/12
H 04 N 7/18 K 7033-5C
8208-3E
G 07 F 7/08 C
Examination requests: Not yet requested
Number of Claims: 5 (Total of 10 Pages)
(54) Title of Invention: ID CARD VALIDITY DETERMINATION SYSTEM AND VALIDITY DETERMINATION APPARATUS
(21) Application No.: HEI 1[1989]-323925
(22) Application Date: December 15, 1989 (Heisei 1)

(72) Inventor:
Hitoshi Nagato
Toshiba Research and Development Center
1 Komukai Toshiba-cho, Saiwai-ku
Kawasaki-shi, Kanagawa Prefecture
(71) Applicant:
Toshiba Corporation
72 Horikawa-cho, Saiwai-ku
Kawasaki-shi, Kanagawa Prefecture
(74) Agent:
Kensuke Norichika [?], patent attorney (and one other party)

[Specification]

1. Title of Invention: ID Card Validity Determination System And Validity Determination Apparatus

2. [Claims]

(1) An ID card validity determination system that, on an ID card created by using a dot printer to record personal data and photographic data, checks changes in the density of image points at least in the main scanning direction or sub-scanning direction of the image points of the photographic data portion, and determines the ID card to be genuine when this period matches the resolution of the printer that recorded

the photographic data and determines the ID card to be false when this [period] does not match.

(2) An ID card validity determination apparatus that uses the ID card validity determination system described in Claim 1; characterized in that it has a photodetector having the capability to resolve resolutions narrower than the minimum resolution of the printer that has created the ID card.

(3) An ID card validity determination system that, in the case of an ID card that has formed at least the photographic data using sublimation dyes, so-called thermal sublimation recording, determines the ID card to be false when the reflected light in the photographic data portion is not nearly uniform through the combination of near infrared light and a photodetector that reacts to near infrared light to generate output.

(4) An ID card validity determination system that records the various portions of the ID card using a number of printers with different resolutions and, when it has read the ID card, checks whether the respective portions match the resolutions of the respective printers and determines that there is a possibility that the ID card is not a fake when a match is obtained for at least one location or more.

(5) An ID card validity determination system that converts personal data based on a special conversion formula, records results based on this conversion in the photographic data portion, performs conversion based on a conversion formula that is already known when it has read the personal data of the ID card, and determines that the ID card is genuine by the fact that that data matches the data read from the photograph portion.

3. [Detailed Explanation of the Invention]
[Purpose of the Invention]
(Field of Industrial Application)

This invention relates to an ID card validity determination system and validity determination apparatus that, on an ID card in which personal data that has been put into character form and a facial photograph of the person in question has been recorded, determines whether or not the personal data is the person shown by the facial photograph.

[Prior Art]

Conventionally, ID cards have been formed by arranging a facial photograph on paper or plastic on which personal data has been printed and laminating these all at once. ID cards are used as employee identification, credit cards, CD cards or cards that prove the identity of an individual. Recorded as personal data on the ID card are the person's name, date of birth, personal identification number (if an employee card, the employee number, etc.), and the issuance number of the ID card as well. These personal data may be made visible, but in some cases they may be recorded in an invisible status as in the case of a magnetic card.

In the past, the amount of ID card usage was not very great, but recently ID cards have come into use in a variety of fields. However, simultaneously with this there has also come to be frequent illegal use relating to these cards. For example, the password, PIN, etc. of the card is found out, and another person's card is used illegally.

[Problems To Be Solved By the Invention]

The person's facial photograph is recorded on the ID card in addition to the personal data. Therefore, by visually comparing the card and the person, one can confirm if the person is using his or her own ID card. (Note that in all subsequent cases the discussion will assume that the recorded personal data is correct. Therefore, the photograph that is affixed to the ID card, and, if the person's face matches, the personal data recorded on the ID card will both be considered to be those of the person in question.) When this type of ID card is used, it is possible to commit forgery by using another person's ID card and affixing only one's own facial photograph to it; for example, the facial photograph portion of FIG. 10(a) is cut out and another person's photograph is put in as in FIG. 10(b) in order to misuse the other person's personal data. For example, if a company were to use this ID card in a work attendance system, it would be possible to penetrate the interior of another company and carry out important confidential information using this forged ID card. With regard to personal data forgery, because personal data consists of numbers, alphabetical characters, etc., special conversions are performed on these numbers and characters, and check codes and the like are created and arranged and inserted inside the personal data, so forgery is difficult. However, for facial photographs,

forgery can be easily achieved by the method of switching to affix another person's facial photograph or the method of photographing the ID card with the other person's facial photograph affixed. The purpose of the present invention is to exhibit a method of determining whether the personal data on an ID card and the facial photograph of the person recorded thereupon are correct or not.

[Configuration of the Invention]

[Means To Solve Problems]

In order to solve the aforementioned problems, the ID card reading system of the present invention is characterized in that it has a means for reading personal data and a means for also reading data that is recorded on the photograph portion, and it is a system for checking whether the data relationship between these is as specified and for checking the validity of the ID card.

[Action]

Because it has such a configuration, by comparing the read personal data or part of this data or data obtained using a certain conversion formula on this personal data with the data read from the photograph portion, it is possible to make determinations such that the ID card is proper if these match, and it is a forged ID card if a mismatch has occurred.

[Embodiments]

- First Embodiment

A number of embodiments of the present invention will be indicated below while referring to drawings. First, in the ID card used in the present invention, it is assumed that data that varies according to the individual, specifically, personal data or facial photograph data are all recorded by a printer. The other common portion is that, even when recorded in advance by printing, when the individual data is recorded, it is permissible to record simultaneously by means of a printer. FIG. 10(a) shows a representative example of an ID card. In this ID card, the configuration uses personal data and facial photograph data. First, the simplest conceivable method of forgery is to cut out the facial photograph or affix another person's photograph on top of it and take a photograph again (FIG. 10(b)). Even if such an ID card were used, with an ordinary checker, only the personal data portion would be checked, so it would be judged to

be genuine. The method of preventing this will be indicated next.

First as the most basic method of checking, a check of the facial photograph portion is performed at the same time, and a check is at least made as to whether or not this facial portion is a composite photograph that has been fit in after the fact. Examples of this method are those that read the facial photograph portion with a sensor inside a checker and make a determination as to whether it has been recorded by a printer or whether the photograph has been fit in. Fortunately, this ID card is recorded by a printer with a uniform resolution, so when enlargement is attempted, the respective image points can be clearly recognized. Specifically, the printer's resolution is from 8 dots/mm to 16 dots/mm, so it would appear that image points of approximately 125 μm to 62.5 μm could be seen (as shown in FIG. 1(a)). In contrast with this, in the case where the facial photograph portion is recorded by a photograph, the silver particles of the photograph are small particles of less than 1 μm. Therefore, when the facial photograph has been checked by a sensor, if it appears that image points equivalent to the resolution of the printer cannot be seen and that the density is continually changing, (as shown in FIG. 1(b)), it is nearly always thought that a photograph has been used, and it can be considered a forged ID card.

Note that there are also cases in which another person's facial photograph is affixed to the ID card and the entirety is photographed to create a forged ID card, so by using a sensor to scan not only the facial photograph but other personal data portions, it is possible to make a determination as to whether the entire ID card has been forged by a photograph according to whether or not image points of the specified resolutions can be observed.

- Second Embodiment

A second embodiment will be shown which determines an ID card to be forged when the facial photograph of the ID card has been replaced with the facial photograph of another person. The facial photograph portion emphasizes gradation, so thermal recording apparatuses that use sublimation color ink are widely used. The ID card used in the present invention is one in which the facial photograph portion is recorded by a color printer that uses thermal sublimation ink. FIG. 2 shows the

reflectivity of magenta ink Thermal sublimation ink is nearly transparent to near infrared light. This is because dyes are used in sublimation ink, which are transparent to near infrared light. Therefore, even if the facial photograph portion were scanned with near infrared light, the reflected light would appear nearly uniform on the sensor. Note that, for the personal data portion, an ink that is mainly pigment is used, so there is sufficient absorption even with near infrared light, and therefore it is possible to read the personal data. In contrast with this, in IDs forged by inserting a photograph, etc. into the face portion, the silver of the photograph portion has sufficient reflective properties even with respect to near infrared light, so signals can be detected when the facial photograph portion is scanned with infrared light. In other words, in the case where a photograph is used in the facial photograph portion and in the case where thermal sublimation ink is used, it is possible to determine the validity of an ID card from the fact that the reflectivity when near infrared light was applied is completely different.

- Third Embodiment

In the second embodiment, a method was shown in which the validity of the ID card was determined by considering the differences in the properties of the ink of the facial photograph portion and the properties of the ink that has recorded the personal data portion, and the present embodiment is also a method that resembles that embodiment. For example, it is a method in which, after recording the facial photograph portion, a special pattern is further printed by fluorescent printing in such a way that visible light is emitted when ultraviolet light is applied. FIG. 3 explains fluorescent ink. The horizontal axis indicates the wavelength, and the vertical axis indicates the absorption or the light emission intensity. As shown in FIG. 3, substances with fluorescent ink absorb ultraviolet light and emit visible light as fluorescent light. Note that, as shown by the dashed line in the drawing, there are also inks that emit fluorescent light in the infrared range. When this type of ink is used, it is sometimes possible to make it completely invisible in the visible light range. In an ID card checker, by applying ultraviolet light, and, for example, reading a visible fluorescent light pattern, and confirming that the determined pattern is recorded at the determined position, it is possible to check the validity

of this ID card. In addition, in this case as well, it is possible to use it together with the first embodiment, etc. and adequately further confirm the validity of the ID card by checking that this fluorescent pattern has also been recorded by a fixed resolution printer.

Note that, in the case where fluorescent recording has been performed, even if a special machine is not used, it is possible to make a determination to a certain extent by viewing under ultraviolet rays. Specifically, when a special fluorescent light pattern is visible, to a certain extent there is a high probability that it is genuine. However, there is also the possibility that it has been forged by fluorescent printing, so it is necessary to use a checker to confirm that image points of the specified resolution are formed.

- Fourth Embodiment

The methods discussed in the embodiments up to this point have used photographs to perform the forgery, but the ID card is also created by a printer, so it is naturally not inconceivable that the forgery could be created using a printer. In such a case, first, a method of making forgery difficult is to vary the resolution of the printer that records the personal data portion and the printer that records the facial photograph. It is, of course, an ID card that has been forged using a printer, so even if the method indicated in the first embodiment were used to check for a forgery, the image points recorded by the printer would be visible, so it would naturally be (mistakenly) determined to be genuine.

Therefore, for example, it is the second embodiment of the present invention that, for example, when the resolution of the printer of the personal data portion and the resolution of the printer for facial photograph recording are varied, and the sensor of the ID card checker is used to read the respective portions, determines validity from the difference in the size of one of the image points generated. For example as shown in FIG. 4, if the personal data portion were recorded by a 10 dots/mm printer, image points of approximately 100 μ could be recorded, or if the facial photograph were recorded by a 12 dots/mm printer, image points of approximately 82.5 μ would be recorded. Therefore, in the case where the resolutions of the printers for recording the personal data portion and the facial photograph portion have been varied in this way, when the personal

data portion and the facial photograph portion have been checked using a sensor, it can be determined to be a forged ID card when recording is performed with image points of the same size.

Note that in this embodiment two printers with different resolutions are used, which are the printer for the personal data portion and the printer for recording the facial photograph, but in the interest of further forgery prevention, it is possible to make the forgery preventing effects greater by varying the respective resolutions using a larger number and a larger variety printers.

- Fifth Embodiment

All of the aforementioned embodiments assume a case where a printer that has exactly the same resolution as the ID card creating equipment and an ink with the same properties could not be prepared, or if it were possible to prepare these, it would be possible to configure equipment to issue ID cards that are basically same as the genuine article. In such a case, for the method of determining the validity of the ID card, that is, the method of determining that the personal data and the person in the facial photograph match, it is necessary to record the personal data or part of it or data created from the personal data basically within the facial photograph as well.

One example of this is the method of recording data created from the personal data within the photograph data, as shown in FIG. 5(a). Of course, this data creation method is such that it is created from personal data as is shown in FIG. 5(b), and only the person creating the ID card knows it, so it is not possible to set it to the appropriate number. That is, it is possible to determine the validity of the ID card by comparing the personal data and the characters in the photograph. However, there is, of course, also a method that uses current photographic technology and printing technology to make the forgery by using another person's photograph and recording identical characters within this photograph. In the case where it is created by photographic technology, by using the first embodiment, it is possible to determine it to be a fake, but in the case where an actual printer has recorded it, it is considerably difficult to determine it to be a forgery.

In such a case, the following type of response is conceivable. For example, it can be such that the four

image points of the upper right of the photograph portion of the ID card of FIG. 5(a) are special image points, for example, they may have weights such as those shown in FIG. 5(c). For example, when the image points are at the 2^0 and 2^3 positions as shown in FIG. 5(c), this indicates 9. And when confirmation data is calculated in FIG. 5(b), the numbers hidden within the image (9, in this case) may be further matched together and calculated. Specifically, the validity of the ID card is checked according to whether or not the confirmation data matches the results of reading in and calculating the personal data and the numbers (characters) hidden within the image with a machine that performs checking of the ID card. That is, it is considerably difficult to check the photographic image and discover a pattern for checking from within this, so it is extremely difficult to forge the ID card. In addition, a sophisticated printer that is able to faithfully reproduce the entire image would be needed.

Note that in the case where a method such as that shown in FIG. 5(c) is used, for the data used in the calculation, it would be sufficient to have only the numbers hidden in the image as shown in FIG. 5(d). There is also hardly any conversion in extreme cases, and it may be output as confirmation data without modification. Also the confirmation data may be displayed by a system such as that shown in FIG. 5(c).

- Sixth Embodiment

If a pattern that is clearly visible to the eye has been recorded within the photograph, a printer may be used to forge it. In order to prevent forgery, a conceivable system would be such that the characters recorded in the photographic image are such that (1) people cannot directly read them when in a normal light ray status. (2) They are recorded in an enciphered status, and other persons are not able to determine where and in what status they are recorded.

(3) By combining (1) and (2) and using a special light beam, the enciphered characters are read from within the photograph portion.

First, as the simplest method, the character string obtained by a special formula from the characters or numbers within the personal data is normally recorded by invisible ink (see FIG. 3). For example, when ultraviolet light is cast, it is conceivable that fluorescent ink that would generate visible light would be used. In

addition, among substances that generate visible light in this way, there are certain cases where the fact they are being recorded becomes known. Therefore, when one would like to keep particularly tight secrecy, it is desirable to use fluorescent ink that would generate infrared fluorescent light when fluorescent light is applied. By doing so, in the normal status, it will be nearly impossible for the characters written in the photograph portion to be recognized. That is, it will become possible to determine the validity using an ID card reading apparatus that has an apparatus that recognizes infrared light and an apparatus that generates ultraviolet rays within one housing.

Note that in this case as well it would be better if the numbers or characters recorded in the photograph portion were not the numbers and characters themselves but specially created character codes and bar codes such as ASCII. Character encoding is also a type of encipherment, but it would be ideal to perform more active encipherment.

- Seventh Embodiment

An example of the method of enciphering personal data and recording it in the facial photograph will be shown. The facial photograph of the ID card emphasizes gradation and resolution, so a sublimation printer is used. Therefore, the respective image points are such that, for example, sub-control of the pulse width of the approximately 128 gradations is performed, and one image point is controlled to 128 gradations. Therefore, for the method of performing enciphering, a method is conceivable in which the strings of numbers and characters obtained from the personal data are replaced with the densities of the respective image points in one portion within the photograph to (encode) and record them. However, in this method, when changes in the ink over time and the fact that the differences in density between the respective gradations are too few is considered, employing it would be too incautious and absurd, and the more one thinks of it, the more it becomes inconceivable.

In order to perform encipherment, it would be optimal to use binary information for whether the image point is present or not. That is, this is a method of using a binary pattern to record by enciphering personal data or a portion thereof or characters, numbers, etc. created from the personal data in one portion within one portion of the photograph. For example, one embodiment of this is

shown in FIG. 6(a). As shown in the figure, data is recorded in the angled portion of the photograph. In this way, the reason that this data is recorded on an angle in a portion of the photograph in this way is, in the case where this data is inserted at the outer edge of the photographic image, to prevent only the photograph portion from being replaced while leaving only this data portion.

We will discuss the system of enciphering as personal data to record in the diagonal line region of the photograph portion. FIG. 6(b) is an example of this. The weights of 2^0, 2^1, 2^2, 2^3, and 2^4 are given according to the respective positions at the four image points in the drawing. This type of pattern is recorded in the diagonal line portion in the photograph of the ID card. For example, if we assume that only the 2^1 and 2^3 positions are recorded at the appropriate density, $2^3 \times 1 + 2^2 \times 0 + 2^1 \times 1 + 2^0 \times 0 = 10$ is expressed. In addition, the portion indicated in the diagonal line portion of FIG. 6(b) is a dummy bit, and it is considered to be recorded at the appropriate density. Also, the data recording start position is set in advance, so data may start to be read from a determined position of this diagonal line portion. Or, a start code indicating the start of writing of the data may be recorded, and the data for confirmation may also be written from there. By doing as indicated above, it is possible to write the personal data of the ID card or a portion thereof or data created from this to a portion of the photograph portion.

Note that the photograph portion is recorded by sublimation ink to which the three colors Y, M and C, or black in addition to these, have been added. As in FIG. 6, the data written in the photograph may be recorded after deciding on one color among these inks. Due to the fact that other inks are dispersed completely randomly, a line in which diagonal confirmation data such as that shown in FIG. 6 is written is recorded. By using a method that writes within this data the data that determines in advance what color of ink the confirmation data is recorded in or that tells what color of data is the confirmation data, or one that varies the ink color in which confirmation data is recorded for each of the respective four image points, it is possible to read the confirmation data that is recorded in the photograph portion. Therefore, by comparing with the results of

reading the personal data portion, it is possible to determine the validity of this ID card.

- Eighth Embodiment

As an embodiment other than the seventh embodiment, there is a method in which the data for confirmation of the ID card is recorded using thermofusible color ink that uses normal pigments. For example, the ID card confirmation data is recorded using thermofusible ink with M pigmentation (FIG. 7(a)). Then, on top of this, the entire surface is colored in diagonal lines as shown in FIG. 7'[sic](b) for example, using thermal sublimation ink with M dying characteristics. That is, by doing so, it is only possible to confirm magenta diagonal lines with the naked eye. Here, when infrared light is used in the ID card reading machine, infrared light is transparent (see FIG. 2) with respect to the dye ink, so the pigment ink is recorded, and it is possible to read only the ID card and the confirmation data hidden under the diagonal lines.

Above, we have indicated a number of methods of determining the validity of an ID card, these are all methods that require a reading apparatus, and the size and configuration of the reading apparatus vary greatly according to the check stage and the importance of the objective of usage. In the most critical locations or in cases of entry to a place where VIPs gather, all of the validity determinations indicated here are, of course, performed, but visual checks and the like must also be performed.

However, this type of stringent check is not normally needed and only a simple check would be sufficient. For example, the most common forgery is the method of inserting one's own photograph into the photograph portion to create a forged ID card. In such a case, it is possible to fulfill the check functions adequately with one or two of these embodiments.

FIG. 8 shows the simplest ID card validity determination apparatus. This apparatus consists of at least an infrared LED array (4) and an infrared CCD array (5). The ID card (7) is moved, for example, in the direction of arrow A, and after the infrared light emitted from the infrared LED array (4) is reflected to the ID card (1), it is incident to the infrared CCD array (5). The character portion (3) is recorded by pigment ink, so infrared light is sufficiently absorbed, and therefore the character pattern recorded in the character

portion (3) is input to the infrared CCD (5). At this time, when the infrared CCD array (5) resolution is made sufficiently small, the resolution of the printer that has recorded the character portion (3) is obtained by a circuit within the apparatus, though this is not shown in the drawing. In cases where this character printer resolution is not as specified, the ID card is determined to be false. An ID card (1) for which a determination has been made that the character portion is genuine is further moved in the direction of arrow A, and the photograph portion (2) comes under an infrared LED (4). If it is a genuine ID recorded by sublimation ink, when the photograph portion (2) has been scanned, the infrared light will be reflected back nearly uniformly to the CCD array sensor (5). Therefore, it is possible to determine that it is a genuine ID card (1) in this case. If the photograph portion (2) has been replaced with another person's photograph, etc., the fact that it is a fake ID card will be quickly ascertained because of changes according to the output photograph pattern from the CCD array (5). A flowchart of the ID card validity determination method resulting from this system is shown in FIG. 9. Note that, if there is leeway, it would be possible to determine the validity of the ID card with considerably high accuracy by calculating the personal data of the read in character portion (3), hiding this calculated value in advance in the photograph portion (2) by the various methods shown in the eight embodiments, and performing a check again when these data have been read in.

[Effects of the Invention]

By using this invention, it is possible to form an ID card determination apparatus that makes it difficult to forge an ID card by putting in personal data and a photograph and that is able to simply determine that an ID card is a fake even if a forged ID could be made.

4. [Brief Explanation of the Drawings]

FIG. 1 is a drawing for explaining the ID card and the first embodiment of the present invention. FIG. 2 is a drawing for explaining the reflection characteristics of dye ink and pigment ink. FIG. 3 is a drawing that explains light absorption and light emission in the case where fluorescent ink is used. FIG. 4 is a drawing for explaining another method of recording the ID card with

printers that have two different resolutions and determining the validity of the ID card by whether the resolution is of the specified size depending on the case. FIG. 5 is a drawing that shows the method of determining the validity of the ID card by recording data, which has been obtained using the personal data, in the photograph portion, reading the ID card, and determining whether or not the value obtained by calculating the personal data matches the data recorded in the photograph portion. FIG. 6 is a drawing that shows the method of recording the confirmation data in the photograph portion. FIG. 7 is a drawing that shows the method of recording this data by thermofusible ink and further using a thermal sublimation ink that is dye to make this data invisible to the naked eye. FIG. 8 is a drawing that shows the simplest example of the ID card validity determination apparatus of the present invention. FIG. 9 is a flow chart of this ID card validity determination apparatus. FIG. 10 is a drawing that shows an example of an ID card (a) and a forged ID card (b) in which the only the photograph portion of the ID card has been replaced.

Agent and patent attorney: Kensuke Norichika
Agent and patent attorney: [Tadayuki] Matsuyama
FIG. 1
FIG. 2
/1/ Reflectivity
/2/ Magenta ink
/3/ Pigment ink
/4/ Dye ink
/5/ Wavelength
/6/ Infrared light
FIG. 3
/1/ Absorption
/2/ Light emission
/3/ Infrared light emission
/4/ Ultraviolet
/5/ Wavelength
/6/ Infrared
FIG. 4

FIG. 5
/1/ Personal data
/2/ Formula
/3/ Secret
/4/ Confirmation data
/5/ Numbers hidden in the image
/6/ Formula
/7/ Confirmation data
FIG. 6
FIG. 7
FIG. 8
1. ID card
2. Photograph portion
3. Character portion
4. Infrared LED
5. Infrared CCD
FIG. 9
/1/ Start of ID card reading
/2/ Character portion resolution check [OK]?
/3/ Image portion sublimation ink check [OK]?
/4/ Genuine ID card
/5/ Fake ID card
FIG. 10

* * *

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-185585

⑤Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成3年(1991)8月13日
G 06 K 17/00	S	6711-5B	
G 07 F 7/12			
H 04 N 7/18	K	7033-5C	
		8208-3E　G 07 F 7/08	C

審査請求　未請求　請求項の数 5　(全10頁)

⑭発明の名称　ＩＤカードの真偽判別方式及び真偽判別装置

⑳特　願　平1-323925
㉒出　願　平1(1989)12月15日

㉑発明者　永戸　一志　神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士 則近 憲佑　外1名

明　細　書

1．発明の名称

ＩＤカードの真偽判別方式及び真偽判別装置

2．特許請求の範囲

(1) パーソナルデータ、および写真データを、ドットプリンタで記録し、作成するＩＤカードに於て、少なくとも写真データ部の画点の主走査方向又は副走査方向の画点の濃度変化を調べ、この周期が、写真データを記録したプリンタの解像度と一致した場合には、真のＩＤカードであり、一致しない場合には、偽のＩＤカードであると判別する、ＩＤカードの真偽判別方式。

(2) 解像度が、ＩＤカードを作成したプリンタの最小解像度より、更に細かく解像できる性能を持った、光検出器を持つことを特徴とする請求項１記載のＩＤカードの真偽判別方式を使用した、ＩＤカード真偽判別装置。

(3) 少なくとも写真データを昇華性染料を使用した、いわゆる熱昇華記録によって形成したＩＤカードの場合には、近赤外光と、近赤外光に反応して出力を生ずる光検出器の組合わせにより、写真データ部での反射光がほぼ一様でない場合には、偽のＩＤカードであると判別するＩＤカードの真偽判別方式。

(4) ＩＤカードの様々な部分を解像度の異なるいくつかのプリンタで記録し、ＩＤカードを読み取った場合に、それぞれの部分が、それぞれのプリンタの解像度と一致しているかを調べ、少なくとも一箇所以上で一致が得られている場合にそのＩＤカードは偽物でない可能性があると判断するＩＤカードの真偽判別方式。

(5) パーソナルデータを特別な変換式に基づいて変換し、写真データ部に、この変換に基づいた結果を記録しておき、ＩＤカードのパーソナルデータを読み取った場合に、予めわかっている変換式に基づいて変換し、そのデータと写真部から読み取ったデータが一致していることによって、真のＩＤカードであると判別するＩＤカードの真偽判別方式。

3．発明の詳細な説明

【発明の目的】

（産業上の利用分野）

この発明は、文字化されたパーソナルデータと、本人の顔写真が記録されたＩＤカードに於て、パーソナルデータが顔写真で示されている人自であるか否かを判定するＩＤカードの真偽判別方式及び真偽判別装置に関する。

（従来の技術）

従来ＩＤカードは、パーソナルデータが印刷された紙あるいはプラスチック上に、顔写真などを合わせ、これらを一括して、ラミネートすることによって形成していた。ＩＤカードは、社員証，クレジットカード，ＣＤカード，あるいは個人を証明するカードとして使用されている。ＩＤカード内にはパーソナルデータとして、本人の名前，生年月日，個人番号（社員証なら、社員番号など）更に、ＩＤカードの発行ナンバーなどが記録されている。これらのパーソナルデータは、可視化されているものもあるが、場合によっては磁気カードのような不可視な状態で記録されているものもある。

従来、ＩＤカードの使用量は、あまり多くなかったが、最近では様々な分野に於て、ＩＤカードが使用されるようになってきた。しかし、これと同時にこれらのカードに関する不正使用も多発するようになってきている。例えばカードのパスワード、暗証番号などを調べだし、他人のカードを不正に使用することなどが行なわれている。

（発明が解決しようとする課題）

ＩＤカードには、パーソナルデータが記録されている他に、本人の顔写真が記録されている。従って、カードと本人を見比べることによって、本人が自分自身のＩＤカードを使用していることが確認できる。（なお、今後全ての場合、記録されているパーソナルデータは正しいのであると仮定した上で話を行っていく。従って、ＩＤカードに貼られてある写真と、本人の顔が一致していればＩＤカードに記録されたパーソナルデータも、本人のものであるとする。）このようなＩＤカードを使用する場合に、他人のＩＤカードを使用し、顔写真だけ自分のものと貼りかえる偽造を行なう、例えば第１０図(a)の顔写真部分を切り取り、(b)のように他人の写真を入れることによって、他人のパーソナルデータを悪用することが可能となる。例えばこのＩＤカードを出退勤管理システムに利用している会社があるとすると、この偽造したＩＤカードで他社内部まで侵入でき、重要な機密情報を持ち出すことなどが可能となる。パーソナルデータの偽造については、パーソナルデータが数字，アルファベットなどで構成されているために、これらの数字や文字に特殊な変換をほどこし、チェックコードなどをつくり出し、パーソナルデータ中に合わせて入れておくため、偽造はむずかしい。しかし、顔写真については、他人の顔写真と貼り変える方法あるいは他人の顔写真を貼った、ＩＤカードを写真で取ってしまう方法などによって、簡単に偽造できてしまう。本発明の目的は、ＩＤカードのパーソナルデータと、そこに記録されている本人の顔写真が正しいものであるかを判断する方法について示すことを本発明の目的としている。

【発明の構成】

（課題を解決するための手段）

上述した問題点を解決するために、本発明のＩＤカードの読み取り方式は、パーソナルデータを読み取る手段と、更に写真部にも記録されているデータを読み取る手段とを持っていることを特徴としており、これらの２つのデータの関係が、規定通りのものであるかどうかを調べ、ＩＤカードの真偽を調べる方式である。

（作　用）

このような構成に成っているために、読み取ったパーソナルデータあるいはこのデータの一部又は、このパーソナルデータをある一定の変換式に基づいて、得られたデータなどと、写真部から読み取ったデータとを比較することにより、これらが一致した場合には、このＩＤカードは正しいカードであるとし、不一致を生じた場合には偽造ＩＤカードであると判別可能となる。

（実施例）

・第１の実施例

以下図面を参照し、本発明の実施例について説明する。まず、本発明で使用するＩＤカードでは、個人によって異なるデータ、つまりパーソナルデータや顔写真のデータは全てプリンタで記録することを前提とする。他の共通部分は、予め印刷で記録してあっても、個人データを記録する際にプリンタで同時に記録してもかまわない。第１０図(a)にＩＤカードの代表例を示す。このＩＤカードでは、パーソナルデータと顔写真で構成されている。まず最も簡単に考えられる偽造法は顔写真の部分を切り取り、又はその上に他人の顔写真を貼りつけ再度写真にとって、行う方法である（第１０図(b)）。このようなＩＤカードを使用しても、通常のチェッカーでは、パーソナルデータ部しかチェックしてないために、本ものと判定してしまう。これを防止する方法を次に示す。

まず最も基本的なチェックの方法としては、顔写真部のチェックも同時に行なって、少なくとも、この顔の部分が後からはめ込まれた合成写真でないことをチェックする方法である。この方法としては、チェッカー内のセンサで顔写真部を読み取り、プリンタで記録されたものか、写真がはめ込まれたものであるかを判定する方法である。幸いなことに本ＩＤカードは解像度の一定なプリンタで記録されているために、拡大してみると各画点がはっきりと確認できる。つまりプリンタの解像度は８ドット／㎜～１６ドット／㎜程度であるので、約１２５μｍ～６２.５μｍ程度の画点が見えるはずである（第１図(a)に示すように）。これに対し、顔写真の部分が写真で記録されている場合には、これに対し、写真の銀粒子は１μｍ以下の小さな粒子である。従って顔写真部をセンサでチェックした場合に、プリンタの解像度に相当する画点が見えず、濃度が連続的に変化しているようであれば、（第１図(b)に示すように）ほぼ写真を使用したものであると考えられ、偽造ＩＤカードであると考えられることができる。

なお、ＩＤカードに他人の顔写真を貼って、全体を写真にとって、偽造ＩＤカードを作る場合もあるので、顔写真ばかりでなく、他のパーソナルデータの部分も、センサでスキャンすることにより規定どおりの解像度の画点が識別できるか、否かによってＩＤカード全体が写真で偽造されたかの判定を行うことが可能となる。

・第２の実施例

ＩＤカードの顔写真が他人の顔写真と入れ換えられた場合に偽造ＩＤカードと、判定する第２の実施例を示す。顔写真の部分は階調性を、重視しているために、昇華性のカラーインクを使用した、熱記録装置が、多く使用されている。本発明に使用しているＩＤカードは、熱昇華性インクを使用したカラープリンタで顔写真部を記録しているものとする。第２図にマゼンタインクの反射率を示す。熱昇華性インクは近赤外光に対しては、ほとんど透明である。昇華性インクには物料が使用されており、近赤外光に対しては透明だからである。従って、顔写真の部分を、近赤外光で、走査しても、センサではほとんど反射光は一様となってしまう。なお、パーソナルデータの部分は、顔料を主体としたインクが使用されているために、近赤外光でも充分な吸収があるために、パーソナルデータを読み取り可能である。これに対し、写真などを顔の部分に入れ込んで、偽造したＩＤカードでは、写真部の銀が、近赤外光に対しても、充分な反射特性を持っているために、顔写真の部分を赤外光で走査すると信号が検出できる。つまり、顔写真の部分に写真を使用した場合と、熱昇華性インクを使用した場合とで、近赤外光を当てた時の反射率が全く異なっていることから、ＩＤカードの真偽が判定できるのである。

・第３の実施例

第２の実施例では、顔写真の部分のインクの特性と、パーソナルデータ部を記録したインクの特性の違いを考慮することによって、ＩＤカードの真偽を判定する方法を示したが、本実施例もこの実施例に似た方式である。例えば顔写真の部分を記録した後に、更に特殊なパターンを、紫外光を当てると可視光を発するけい光印刷によって印刷する方法もある。第３図にはけい光イ

ンクを説明してある。横軸は波長たて軸は吸収又は発光強度を表わしている。けい光インクのあるものは、第3図のように紫外光を吸収し可視光をけい光として発している。なお図で破線で示すように、赤外域にけい光を発するインクもある。このようなインクを使用すると可視光領域では全く見えなくなることも可能である。ＩＤカードのチェッカでは、紫外光を当てて、例えば可視光のけい光パターンを読み取り、定められた位置に定められたパターンが記録されていることを確かめることで、このＩＤカードの真偽をチェックすることができる。更にこの場合にも第１の実施例などといっしょに使用し、このけい光パターンも一定の解像度のプリンタで記録されたことを、チェックすることによって、更にＩＤカードの真偽性を充分に確保することが可能となる。

なお、けい光記録を行った場合には特殊な媒体を使用しなくても、紫外線の下で見ることによって、ある程度の判定は可能である。つまり、特殊なけい光パターンが見える場合にはある程度、本物である可能性が高い。しかし、けい光印刷で偽造した可能性もあるので、チェッカによって、指定の解像度の画点が形成されているか確認する必要がある。

・第４の実施例

今までの実施例で述べた方法では写真を使用して、偽造を行う方法であるが、ＩＤカードもプリンタで作成したものであるので、当然のことながらプリンタを使用しての偽造も考えられないことはない。このような場合には、まず偽造をしにくくする方法として、パーソナルデータ部を記録するプリンタと、顔写真を記録するプリンタの解像度を変えておく方法がある。当然プリンタを使用して、偽造したＩＤカードであるので、第１の実施例で示した方法で偽造を確認しようとしても、プリンタで記録した画点が見えるので、当然本ものと判定してしまう。

そこで、例えばパーソナルデータ部のプリンタの解像度と、顔写真記録用プリンタの解像度を変化させておき、ＩＤカードチェッカーのセンサで、それぞれの部分を読み取った場合に、生ずる１つの画点の大きさの違いから真偽を判定するのが、本発明の第２の実施例である。例えば、第４図の示す様にパーソナルデータ部が１０ドット／㎜のプリンタで記録されているとすると、約１００μ程度の画点が記録でき、また顔写真が１２ドット／㎜のプリンタで記録されているとすると、約８３.３μ程度の画点が記録されることになる。従ってこのようにパーソナルデータ部と、顔写真部記録用のプリンタの解像度を変化させてある場合には、パーソナルデータ部と顔写真部をセンサでチェックした場合に、同じ大きさの画点で記録されているとなると、偽造ＩＤカードであると判定できる。

なお、この実施例では、パーソナルデータ部用プリンタ、顔写真記録用プリンタと、解像度の異なる２台のプリンタを使用しているが、より偽造防止を考えるためには、より多数、多種類の、プリンタを使用して、それぞれの解像度を変えておくことによって、偽造防止の効果を大きくすることができる。

・第５の実施例

以上の実施例ではＩＤカード作成機と全く同様の解像度を持ったプリンタ、同じ特性を持ったインクなどが、用意できなかった場合が全て問題となっているか、これらが用意できれば基本的には本物と同じＩＤカード発行器を構成できるはずである。この様な場合に、ＩＤカードの真偽を判定する方法、すなわちパーソナルデータと顔写真の人物との一致を判定する方法としては、基本的には顔写真の中にも、パーソナルデータ又はこの一部あるいは、パーソナルデータより作成されるデータが記録されている必要がある。

１例をあげると、第５図(a)に示すように写真データの中に、パーソナルデータより作成されるデータを記録する方法である。もちろん、このデータの生成方法は、パーソナルデータから第５図(b)のように作成し、ＩＤカードの製作者以外は知らないので適当な数にすることはできない。つまり、パーソナルデータと写真中の文字を比較

するとによって、ＩＤカードの真偽の判定が可能となるわけである。ただし、もちろん、現在の写真技術や、プリント技術を用いることによって、他人の写真を使用し、この写真の中に同一の文字を記録して、偽造してしまう方法もある。写真技術で作った場合には第１の実施例を使用することで、にせものと判断することができるが、高価のプリンタで記録された場合には、偽物と判断することはかなりむずかしい。

このような場合には、以下のような対応が考えられる。例えば第５図(a)のＩＤカードの写真部の右上の４つの画点は特別な画点であり、例えば第５図(c)のような並びを持っているものとする。例えば第５図(c)のように2^0と2^3の位置に画点があるとすると、これは、９を表わしている。そこで第５図(b)で暗証データを計算する場合に、更に画像の中に隠されている数字（この場合は９である）を、一緒に合わせて計算すれば良い。つまりＩＤカードのチェックを行う装置で、パーソナルデータと画像中に隠された数字（文字）を読み込み計算した結果が、暗証データと一致しているか否かによってＩＤカードの真偽をチェックする。つまり写真画像を詳しく調べて、この中からチェック用のパターンを見つけることはかなり困難であるので、ＩＤカードを偽造が非常に困難となる。また、全画素を忠実に再現できる精巧なプリンタが必要となる。

なお第５図(c)のような方法を使用する場合には計算に用いるデータとしては第５図(d)のように画像中に隠されている数字だけでも充分である。簡単な場合には変換もほとんどしないで、そのまま暗証データとして出力しても良い。また暗証データも、第５図(c)に示すような方式で表示してもよい。

・第５の実施例

明らかに目に見える装飾を写真の中に記録しておいたのでは、プリンタを使用することによって偽造されてしまう。偽造防止するためには、写真画像中に記録されている文字が

① 普通の光線状態では、人間は識別できない。

② 暗号化された状態で記録されており、どこに、どのような状態で記録されているのか、他人には判別できなくする。

③ ①と②を合わせ、特殊な光線を使用することによって、写真部の中から、暗号化された文字を読み出す。

などの方式が考えられる。

まず最も簡単な方法としては、パーソナルデータ内にある文字あるいは数字から、特殊な計算式によって得られた文字列を、通常では、見えないインクで記録する方法である（第３図参照）。例えば紫外光をあてると、可視光を発生するようなけい光インクを使用することが考えられる。また、このように可視光を発生するものでは、ある場合には記録されていることがわかってしまう場合もある。そこで、特に秘密を厳守したい場合には、紫外光を与えると、赤外光のけい光を発するような、けい光インクを使用することが望ましい。このようにすることによって通常の状態では、写真部に含まれた文字を認識することはほとんど不可能である。つまり、紫外光を発生する装置と、赤外光を認識する装置を１つの筐体の中に持ったＩＤカードの読み取り装置によってその真偽の判定が可能となるわけである。

なお、この場合にも写真部に記録される数字あるいは文字は、数字・文字そのものでなく、ＡＳＣＩＩなど、あるいは特別に作った文字コード、バーコードなどであった方が良い。文字のコード化も一種の暗号化であるが、更により積極的に暗号化を行なった方が理想的ではある。

・第７の実施例

パーソナルデータを暗号化して顔写真の中に記録する方法の１例を示す。ＩＤカードの顔写真は、階調性と解像度を重視しているために、昇華性プリンタが使用されている。従って各画点は例えば１２８階調程度のパルス幅制御が行なわれており、１つの画点は１２８階調に制御される。そこで暗号化する方法としては、写真の中の一部分に、パーソナルデータから得られる文字・数字列を、各画点の濃度に置き換えて、（暗号化）し

て記録しておく方法が考えられる。しかしこの方法では、インクの経時変化や各階調間の濃度差があまりにも小さすぎることを考えると、採用するには、あまりにも無謀で、あぶらしすぎて、何か考えているとは考えられない状況である。

暗号化するためには、画点があるか否かの2値の情報を使用するのが最適である。つまり、写真の中の一部分に、2値のパターンで、パーソナルデータあるいはその一部又は、パーソナルデータから作成される文字・数字などを暗号化して記録する方法である。例えば第6図(a)にその実施例の1つを示す。図のように写真の一部の斜めの部分にこのデータを記録するのである。このように、写真の一部に斜めにこのデータを記録しているのは、写真画像の外枠にこのデータを入れた場合には、このデータ部だけ残して写真部だけ入れ換えられることを防止するためである。

パーソナルデータと暗号化して、写真部の斜線領域に記録する方式について述べる。第6図(b)がその一例である。この図の4つの画点にはそれぞれの位置に応じて2^0，2^1，2^2，2^3の4つの重みが与えられている。このようなパターンをIDカードの写真中の斜線部に記録しておく。例えば2^1，2^3の位置だけが適当な濃度で記録されているとすると、$2^1\times1+2^2\times0+2^1\times1+2^0\times0=10$を表わしていることになる。また第6図(b)の斜線部で示される部分は、ダミーのビットであり、適当な濃度で記録されているとする。またデータの記録開始位置は、予め定められているので、この斜線部の決められた位置からデータを読み始めれば良い。あるいは、データを書き始めてあるというスタートコードを記録しておき、そこから確認用データが書き込まれているとなっていてもよい。以上のようにすることによって、IDカードのパーソナルデータ又はその一部あるいは、これから生成されるデータを、写真部の一部に書き込むことができる。

なお、写真部は、Y，M，Cの3色あるいはこれに更に黒を加えた、昇華性のインクで記録されることになる。第6図のように写真中に書き込まれたデータは、これらのインクのどれか1色を決めて記録しておけば良い。他のインクは全く無秩序に分散させることによって、第6図に示した様な斜めの確認データを書き込まれたラインが記録される。予め何色のインクで確認データを記録してあるのかを決めておく、あるいは、何色のデータが確認データであるかというデータをこのデータの中に書き込んでおく、又は各4画点毎に確認データを記録してあるインクの色を変えてゆくなどの方法を使用することによって、写真部に記録してある、確認データを読み取ることができる。そして、パーソナルデータ部を読み取った結果と比較することによって、このIDカードの真偽を判定することができることになる。

・第3の実施例

第1の実施例の別の実施例の1つとして、IDカードの確認用のデータは通常の顔料を用いた熱溶融性のカラーインクで記録する方法がある。例えば、IDカード確認用のデータをMの顔料性の熱溶融性インクで記録する（第7図(a)）。そして更にこの上に今度は同じMの染料性の昇華性インクで例えば第7′図(b)に示した様に、全面を斜線で塗ってしまう。つまり、このようにすることで、肉眼ではマゼンタの斜めのラインが確認できるだけである。ここでIDカードの読み取り機で赤外光を使用すると、染料インクに対して赤外光は透明である（第2図参照）ので、顔料インクが記録されて、斜線の下に隠されていたIDカード，確認用のデータだけを読み取ることが可能となる。

以上、幾つかのIDカードの真偽を判別する方式について示してきた。これらはいづれも読み取り装置を必要とする方法であり、チェックの段階によって、あるいは使用目的の重要度によっては読み取り装置の大きさや価格も大きく異なる。最も重要な場所や、VIP級の人間の集まるような場所へ入場する場合には、ここに示した全ての真偽判別法を行うことはもちろん、目視によるチェック等も充分に行なわなければならない。

しかし、通常はこのような厳重なチェックは必

貫徹く、簡単なチェックだけで充分である。例えば最も多い偽造としては、写真部に自分の写真を入れて偽造ＩＤカードを作る方法などが考えられる。このような場合には、本実施例の１および２項度のチェックでも充分に、チェック機能をはたすことが可能である。

第８図に最も簡単なＩＤカードの真偽判別装置を示す。この装置は、少なくとも赤外ＬＥＤアレイ(4)と赤外ＣＣＤアレイ(5)から構成されている。ＩＤカード(1)は例えば矢印Ａのような方向に動き、赤外ＬＥＤアレイ(4)から出た赤外光はＩＤカード(1)に反射した後、赤外ＣＣＤアレイ(5)へと入射する。文字部(3)は顔料インクで記録されているので赤外光は充分吸収されるので、赤外ＣＣＤ(5)には、文字部(3)に記録されている文字パターンが入力される。この時赤外ＣＣＤアレイ(5)の解像度を充分小さくしておくと、文字部(3)を記録したプリンタの解像度が、図示してはないが装置内の回路によって求められる。この文字プリンタの解像度が規定通りでない場合には、このＩＤカードは偽物と判定される。文字部が本物であると判定されたＩＤカード(1)は、更に矢印Ａの方向に移動され、写真部(2)が赤外ＬＥＤ(4)の下に来る。昇華性インクで記録された本物のＩＤカードであれば写真部(2)を通過した場合には、ＣＣＤアレイセンサ(5)には、赤外光がほとんど一様に反射して返ってくる。従ってこの場合には本物のＩＤカード(1)であると判定できる。写真部(2)を他人の写真等に入れ換えた場合にはＣＣＤアレイ(5)からの出力写真パターンによって変化するので偽物のＩＤカードであると、すぐにわかる。この方式によるＩＤカードの真偽判定法のフローチャートを図９に示す。なお、余裕のある場合には、読み込んだ文字部(3)のパーソナルデータを計算し、実施例の３に示した様な方法でこの計算値を予め写真部(2)の中へ印しておき、これらのデータを読み込んだ時に再びチェックすることを行えばかなり高い精度で、ＩＤカードの真偽の判定ができる。

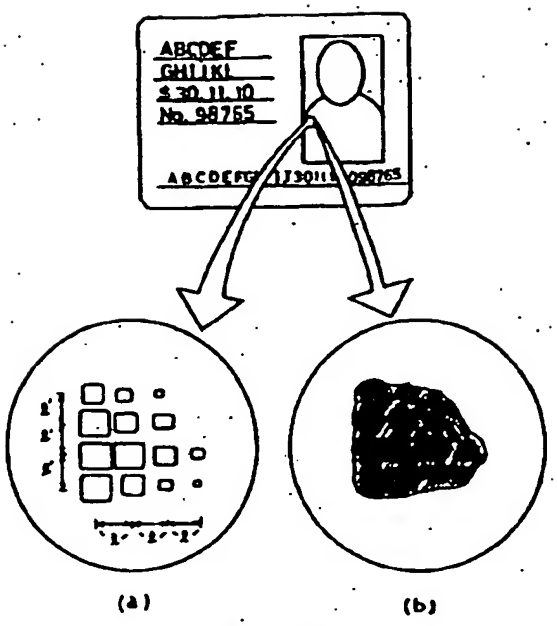
【発明の効果】

この発明を用いることにより、パーソナルデータと写真入りのＩＤカードの偽造を困難とし、もし偽造されたＩＤカードが作られたとしても、簡単に、偽物のＩＤカードであると判定できるＩＤカード判定装置を構成することが可能となる。

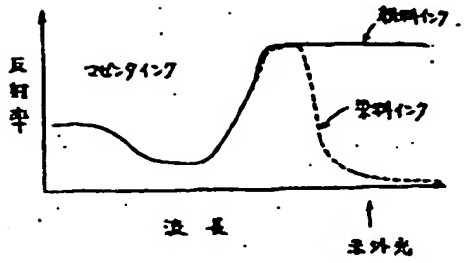
4．図面の簡単な説明

第１図は、ＩＤカードと、本発明の第１の実施例を説明するための図，第２図は熱料インクと顔料インクの反射特性を説明するための図，第３図は、けい光インクを使用した場合の光の吸収と発光を説明した図，第４図は、ＩＤカードを２つの異なった解像度のプリンタで記録し、場所によって規定通りの大きさの解像度になっているか否かで、ＩＤカードの真偽を判別する方法を説明するための図，第５図はパーソナルデータを用いた計算から求めた、データを写真部分に記録しておき、ＩＤカードを読み込んでパーソナルデータを計算した値が、写真部分に記録されているデータと一致するか否かによってＩＤカードの真偽を判別する方法を示す図，第６図は、暗証用のデータを写真部に記録する別の方法を示す図，第７図は熱溶融性インクでこのデータを記録し、更に熱料である熱昇華性インクを使用して、肉眼ではこのデータを見えなくする方法を示す図，第８図は本発明のＩＤカード真偽判別装置の最も簡単な例を示す図，第９図はこのＩＤカード真偽判別装置のフローチャート，第１０図はＩＤカード(a)とその写真部だけを入れ換えた偽造ＩＤカード(b)の例を示す図である。

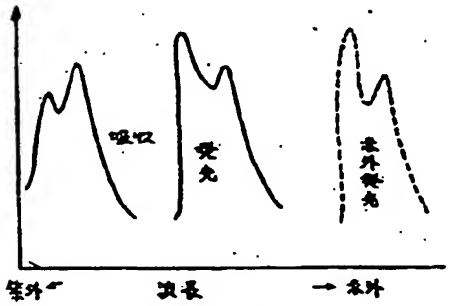
代理人弁理士　則近憲佑
同　　松山允之



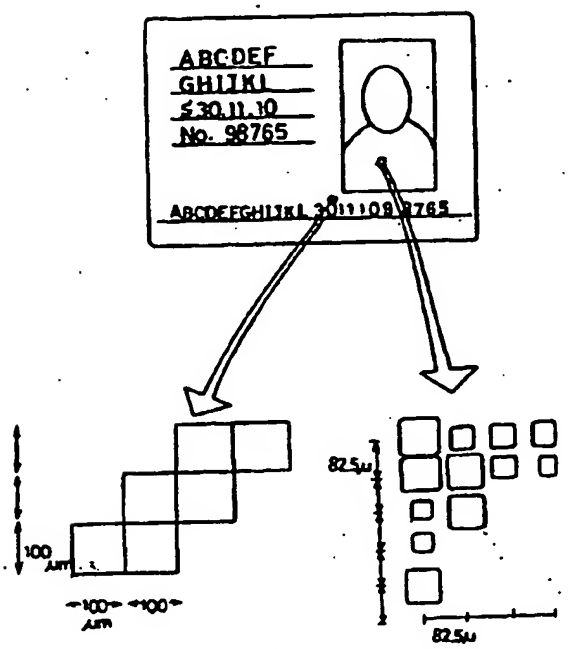
第 1 図



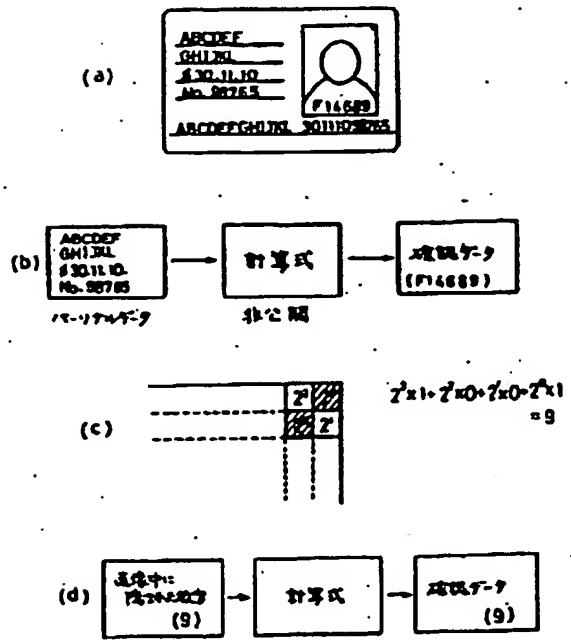
第 2 図



第 3 図

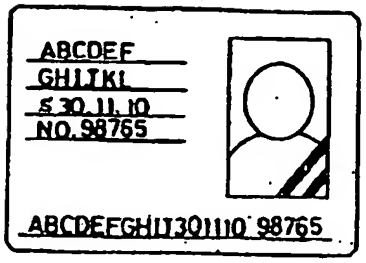


第 4 図

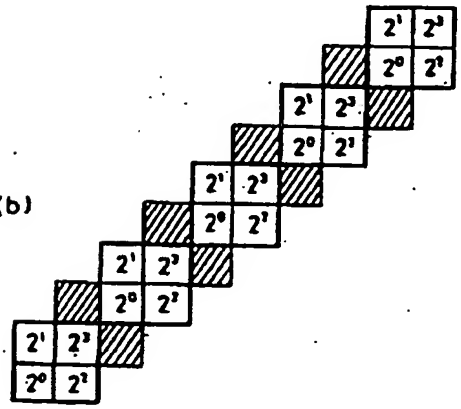


第 5 図

(a)

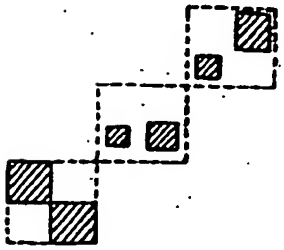


(b)

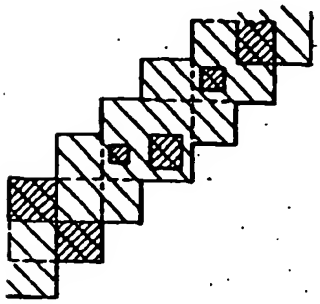


第 6 図

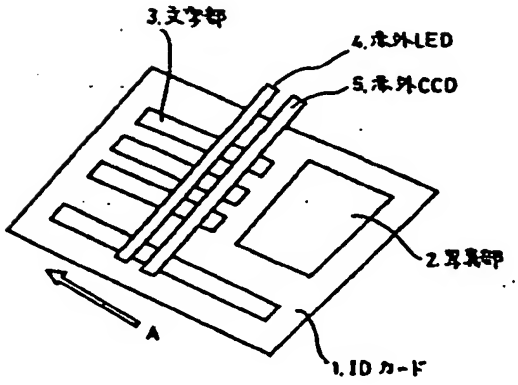
(a)



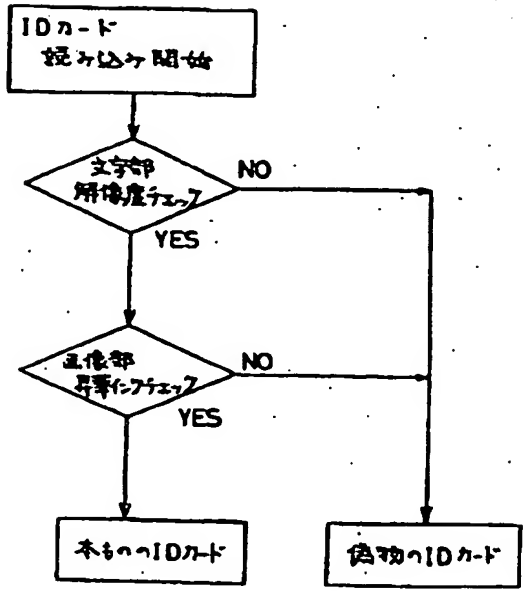
(b)



第 7 図

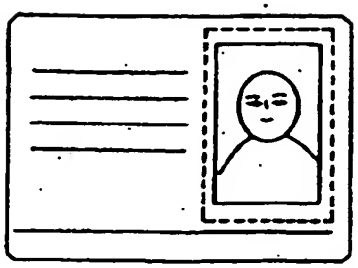


第 8 図

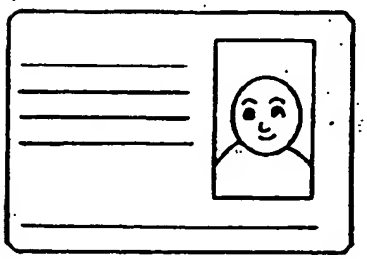


第 9 図

(a)



(b)



第 10 図